รายงานการวิจัยฉบับสมบูรณ์

การประยุกต์สัญญาณอลวนเพื่อสร้างความมั่นคงแก่ข้อมูลความลับสำหรับใช้ในสามจังหวัดชายแดนภาคใต้

Applications of Chaotic Signals for Retaining Confidential Data using in Three-deep Southern Provinces of Thailand

รศ. ดร. ปีติเขต สู้รักษา (หัวหน้าโครงการ)
ผศ. กฤดากร กล่อมการ
เจตน์ ออสวัสดิ์
ศักดา สาครนันท์

ได้รับทุนสนับสนุนงานวิจัยจากเงินงบประมาณแผ่นดินหรือรายได้
ประจำปีงบประมาณ 2553

คณะวิศวกรรมศาสตร์
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

บทคัดย่อ (เงินงบประมาณแผ่นดิน)

ชื่อโครงการ (ภาษาไทย) การประยุกต์สัญญาณอลวนเพื่อสร้างความมั่นคงแก่ข้อมูลความลับสำหรับใช้ใน สามจังหวัดชายแดนภาคใต้

ชื่อโครงการ(ภาษาอังกฤษ) Applications of Chaotic Signals for Retaining Confidential Data using in Three-deep Southern Provinces of Thailand

แหล่งเงิน งบประมาณแผ่นดิน

ประจำปีงบประมาณ 2553 จำนวนเงินที่ได้รับการสนับสนุน 575,000 บาท

ระยะเวลาทำการวิจัย 1 ปี ตั้งแต่ 1 ตุลาคม 2552 ถึง 30 กันยายน 2553

ชื่อ-สกุล หัวหน้าโครงการ และผู้ร่วมโครงการวิจัย พร้อมระบุ หน่วยงานต้นสังกัดและ อีเมล์

รศ. ดร. ปิติเขต สู้รักษา (หัวหน้าโครงการ) คณะวิศวกรรมศาสตร์ สจล. kspitikh@kmitl.ac.th

ผศ. กฤดากร กล่อมการ คณะวิศวกรรมศาสตร์ สจล. kkkitdak@kmitl.ac.th

เจตน์ ออสวัสดิ์ คณะวิศวกรรมศาสตร์ สจล. kojedt@gmail.ac.th

ศักดา สาครนันท์ คณะวิศวกรรมศาสตร์ สจล. sakornsa@hotmail.com

คำสำคัญ (Keywords) สัญญาณอลวน รหัสลับ ความมั่นคงข้อมูล สามจังหวัดชายแดนภาคใต้

บทคัดย่อ

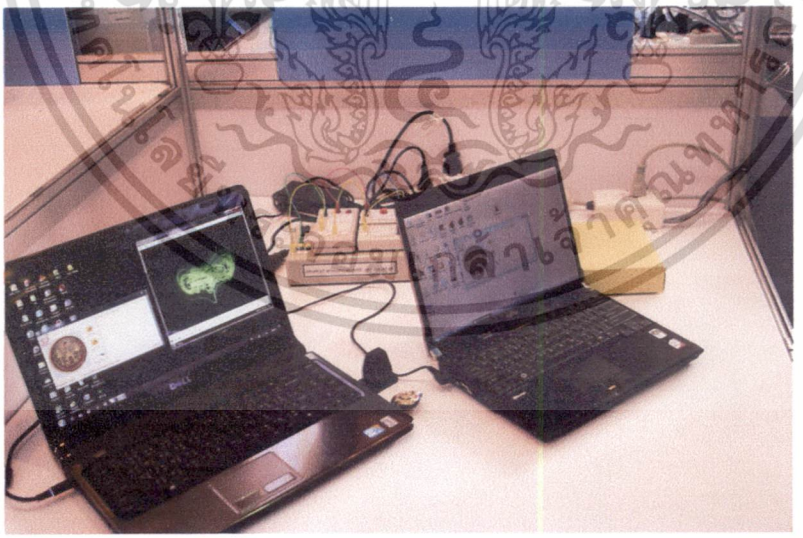
ปัญหาการปลอมแปลงเอกสารลับของราชการจากการลักลอบเข้าใช้ระบบเครือข่ายอื่น ๆ เป็นที่มาของปัญหาในงานวิจัยนี้ งานวิจัยนี้ แสดงตัวอย่างของการป้องกันการปลอมแปลงตัวบุคคลเพื่อเข้าใช้ระบบดังกล่าวข้างต้น ตัวอย่างที่แสดงคือการเข้ารหัสลับข้อมูล วิธีการที่ใช้ในงานนี้วิจัยนี้เป็นการประยุกต์สัญญาณอลวนเพื่อเข้ารหัสลับข้อมูลในการส่งผ่านระบบเครือข่ายคอมพิวเตอร์ ผลการทดลองที่ได้สาธิตความเป็นไปได้สูงในการขยายผลสู่การประยุกต์ขั้นภาคสนามในการใช้งานจริงต่อไป

Abstract

Problems of authentication has been attracted much attention due to crackers may crack into the networks for stealing government's confidential document. Thus the problem is a motivation of this research in order to prevent such an action performed by the unauthorized. To illustrate an example, encryption for confidential document via the computer network is carried out. The experimental results show high potential to extend this work for operation in real-world application.

รูปภาพผลงานวิจัย (output) และผลลัพธ์ (outcome)

รูป ก ผลลัพธ์จากงานวิจัยนี้ที่ได้รางวัลยอดเยี่ยมประเภทต้นแบบนวัตกรรมโทรคมนาคม ประจำปี พ.ศ. 2553 จากสถาบันวิจัยและพัฒนาอุตสาหกรรมโทรคมนาคม (TRIDI) สำนักงานคณะกรรมการกิจการโทรคมนาคมแห่งชาติ



รูป ข อุปกรณ์การเข้ารหัสลับด้วยสัญญาณอลวนประกอบด้วยสองส่วนคือ “what-we-know” **คือส่วนของซอฟท์แวร์และรหัสผ่าน** (password) **กับส่วน** “what-we-have” **คือส่วนของฮาร์ดแวร์เสียบที่ช่อง** USB

กิตติกรรมประกาศ

งานวิจัยนี้ สำเร็จลงได้ด้วยเงินอุดหนุนงบประมาณแผ่นดินประจำปี 2553 หากไม่ได้รับการสนับสนุนครั้งนี้ คงไม่มีผลลัพธ์จากงานวิจัยนี้ที่ได้รางวัลยอดเยี่ยมประเภทต้นแบบนวัตกรรมโทรคมนาคม ประจำปี พ.ศ. 2553 จากสถาบันวิจัยและพัฒนาอุตสาหกรรมโทรคมนาคม (TRIDI) สำนักงานคณะกรรมการกิจการโทรคมนาคมแห่งชาติ

คำนำ

คณะผู้วิจัยหลัก ได้เล็งเห็นความสำคัญของการจัดการเอกสาร การเข้าถึง และการรักษาข้อมูลที่เป็นความลับของชาติ ด้วยความจำเป็นดังกล่าวการสร้างความมั่นคงให้ข้อมูลความลับด้วยเทคโนโลยีที่สร้างด้วยองค์ความรู้ของตนเองจึงมีความสำคัญยิ่ง ซึ่งการซื้อเทคโนโลยีการเข้ารหัสลับมาจากต่างประเทศนั้นเปรียบเสมือนการซื้อใช้ชุดกุญแจที่สร้างโดยผู้อื่น จึงไม่ต้องสงสัยเลยว่าผู้ผลิตย่อมสามารถสร้างลูกกุญแจกี่ลูกก็ได้ในการไขแม่กุญแจที่ซื้อมาล๊อกประตูบ้าน

งานวิจัยนี้ เป็นจุดเริ่มต้นของการปกป้องทรัพย์สินทางปัญญาของประเทศไทยในศาสตร์รหัสลับวิทยาอันมีการประยุกต์และใช้งานอย่างมากในช่วงสงครามยุคต่าง ๆ โดยเฉพาะอย่างยิ่งในช่วงสงครามโลกครั้งที่ 2 ซึ่งการออกแบบและประยุกต์ใช้รหัสลับในรูปแบบต่าง ๆ นั้นนักคิดมักเกิดในโลกตะวันตก และรหัสลับระดับสูงนั้นจัดเป็นยุทธปัจจัยมีข้อจำกัดในการส่งออก ดังนั้นจึงจำเป็นที่องค์ความรู้นี้ควรสร้างเองด้วยเหตุผลดังกล่าวข้างต้น ซึ่งผลงานวิจัยนี้ได้ส่งมอบให้กับหน่วยงานในสามจังหวัดชายแดนภาคใต้เพื่อนำไปใช้ประโยชน์ในภาคสนาม

อนึ่ง เนื้อหาของงานวิจัยโดยเชิงละเอียดในฉบับนี้ คณะผู้วิจัยขอสงวนสิทธิไม่ลงรายละเอียดเนื่องจากเหตุผลทางด้านความมั่นคงทางการข่าวและข้อมูลเชิงการทหาร

ปิติเขต สู้รักษา
(หัวหน้าโครงการ)

สารบัญ

หน้า

สารบัญรูป

รูปที่ **หน้า**

บทที่ 1 บทนำ

1.1 ที่มาและความสำคัญของปัญหา

จากปัญหาการปรากฏของเอกสารลับราชการชิ้นหนึ่งซึ่งเป็นไปในชั้นความลับได้ปรากฏในอินเตอร์เนต ดังรูปที่ 1 เปิดประเด็นถกเถียงในเรื่องของการพิสูจน์ตนว่าเป็นเอกสารจริงหรือทำขึ้น อย่างไรก็ตาม ไม่ว่าผลการพิสูจน์จะทำในรูปแบบใด หากเอกสารนี้เป็นเอกสารจริง จะก่อให้เกิดความเสียหายต่อประเทศชาติได้

รูปที่ 1 เอกสารลับ “คมช.” ที่มา http://203.150.225.235/view/17349/8

คณะผู้วิจัยหลัก ได้เล็งเห็นความสำคัญของการจัดการเอกสาร การเข้าถึง และการรักษาข้อมูลที่เป็นความลับของชาติ ด้วยความจำเป็นดังกล่าวการสร้างความมั่นคงให้ข้อมูลความลับด้วยเทคโนโลยีที่สร้างด้วยองค์ความรู้ของตนเองจึงมีความสำคัญยิ่ง ซึ่งการซื้อเทคโนโลยีการเข้ารหัสลับมาจากต่างประเทศนั้นเปรียบเสมือนการซื้อใช้ชุดกุญแจที่สร้างโดยผู้อื่น จึงไม่ต้องสงสัยเลยว่าผู้ผลิตย่อมสามารถสร้างลูกกุญแจกี่ลูกก็ได้ในการไขแม่กุญแจที่ซื้อมาล๊อกประตูบ้าน

สำหรับ อุปกรณ์เข้ารหัสลับที่มีความแข็งแกร่งสูงนั้น นอกจากจะมีราคาสูงมากต่อเครื่อง ยังถูกควบคุมโดยใกล้ชิดจากรัฐบาลของผู้ผลิตสำหรับอนุญาตให้ใช้สำหรับบุคคลในประเทศและห้ามส่งออกเครื่องมือนี้ไปยังต่างประเทศ อีกทั้งยังต้องมั่นใจให้

ได้ว่าหน่วยงานของรัฐมีศักยภาพสูงพอที่จะถอดรหัสโดยปราศจากกุญแจเข้ารหัส (Cryptanalysis) ของอุปกรณ์เหล่านี้ได้ และสำหรับอุปกรณ์ที่มีจำหน่ายในตลาดที่สามารถเข้าได้ก็ถูกครอบคลุมโดยสิทธิบัตร สำหรับการพัฒนาอุปกรณ์หรือเครื่องป้องกันการเจาะข้อมูลความลับที่เสนอในข้อเสนอโครงการวิจัยนี้อยู่บนพื้นฐานของการประยุกต์ใช้ทฤษฎีอลวน (chaos theory) ในการเข้ารหัสลับของไฟล์พหุสื่อ (multi-media) โดยสัญญาณอลวนในงานวิจัยนี้จะมุ่งค้นคว้าพัฒนาในรูปแบบที่มีความปลอดภัยสูงสุดแก่กองทัพและหน่วยงานตำรวจและหน่วยงานความมั่นคงของชาติ อีกทั้งขยายผลครอบคลุมกลุ่มผู้ต้องการความปลอดภัยข้อมูลระดับกลางได้แก่บริษัทหรือองค์กรการค้า การธนาคารของประเทศไทย รวมทั้งระดับรักษาความปลอดภัยข้อมูลเบื้องต้นคือระดับผู้ใช้งานส่วนบุคคลทั่วไปที่ต้องการความเป็นส่วนตัวและรักษาข้อมูลเพื่อไม่ให้มิจฉาชีพที่เจาะระบบคอมพิวเตอร์นำไปใช้ประโยชน์ในทางมิชอบ

ความพยายามในการป้องกันปัญหาดังกล่าวข้างต้น เป็นแรงจูงใจของงานวิจัยนี้ ซึ่งทางคณะผู้วิจัยมีองค์ความรู้ในการสร้างสัญญาณอลวนที่ค้นพบใหม่ในงานวิจัยนี้ ซึ่งจะได้กล่าวถึงในบทที่ 2 จึงต้องการขยายองค์ความรู้ดังกล่าวสู่การประยุกต์กับการป้องกันการปลอมแปลงตัวบุคคลและเอกสารสิทธิต่าง ๆ ตัวอย่างหนึ่งในงานวิจัยนี้ เป็นการเข้ารหัสและถอดรหัสโดยอาศัยส่วนที่เป็น “what-we-know” ได้แก่ password และ “what-we-have” ได้แก่อุปกรณ์เข้ารหัสลับ เป็นเงื่อนไขเบื้องต้นในการประกอบฟังก์ชันเพื่อสร้างสัญญาณอลวนเพื่อเข้ารหัสดังกล่าว ซึ่งจะได้กล่าวถึงในบทที่ 3

การอภิปรายผลและวิจารณ์ผลการทดลองที่ได้แสดงในบทที่ 4 อภิปรายความเป็นไปได้อย่างสูงที่จะขยายผลการวิจัยที่ได้สู่การนำไปใช้งานจริงทั้งในส่วนภาคเอกชนและส่วนที่เป็นไปเพื่อพัฒนาศักยภาพของกองทัพไทยและการรักษาความสงบภายในเพื่อกิจการกรมตำรวจซึ่งแสดงไว้ในบทสุดท้าย สำหรับบทสุดท้ายหรือบทที่ 5

ในงานวิจัยนี้ เป็นงานวิจัยประยุกต์ทางวิศวกรรมศาสตร์ที่มุ่งเน้นการสร้างต้นแบบโดยมีวัตถุประสงค์ดังแสดงในหัวข้อถัดไป

1.2 วัตถุประสงค์ของการวิจัย

1.2.1 เพื่อสร้างสัญญาณอลวนชนิดใหม่ที่ให้ความปลอดภัยในข้อมูลสูงสุดเพื่อใช้งาน

1.2.2 นำสัญญาณอลวนที่ได้ในข้อ 1.2.1 มาประยุกต์สร้างความมั่นคงให้ข้อมูลความลับ

1.2.3ส่งมอบชิ้นงานและซอฟท์แวร์ที่ได้ในข้อ 1.2.2 แก่หน่วยงานความมั่นคงที่เกี่ยวข้องกับการสร้างและรักษาความสงบในสามจังหวัดชายแดนภาคใต้

1.3 ขอบเขตของโครงการวิจัย

ในงานวิจัยนี้ ครอบคลุมการสร้างสัญญาณอลวนที่ให้ความปลอดภัยสูงสุดเพื่อนำมาใช้ต่อการเข้ารหัสลับและใช้กับพหุสื่อ โดยให้มีความยากต่อการถอดรหัสโดยปราศจากกุญแจ และครอบคลุมถึงการสร้างรหัสลับเพื่อให้ครอบคลุมถึงพหุสื่อในเวลาจริง

บทที่ 2 เอกสารและงานวิจัยที่เกี่ยวข้อง

ตัวดึงดูดอลวน ค้นพบโดยบังเอิญโดย ศาสตรจารย์ Edward N. Lorenz [1] นักอุตินิยมวิทยาแห่งสถาบันเทคโนโลยีแห่งรัฐแมซซาซูเซท ในปี พ.ศ. 2506 โดยเวลานั้น Lorenz ได้พยายามสร้างแบบจำลองทางอุตุนิยมวิทยาด้วยสมการอนุพันธ์แบบไม่เป็นเชิงเส้นขนาดลำดับ 3 ตัว x, y, z ของความสัมพันธ์ระหว่าง อุณหภูมิ ความกดอากาศ ความเร็วลมโดยในสมการมีตัวแปรแบบไม่เป็นเชิงเส้น(quadratic nonlinear) อยู่ 2 เทอม และให้ประมวลผลบนคอมพิวเตอร์ โดยเริ่มประมวลผลด้วยทศนิยม 6 หลัก แต่เนื่องจากขณะนั้นคอมพิวเตอร์มีประสิทธิภาพต่ำ Lorenz จึงได้ลดหลักทศนิยมของค่าเริ่มต้นของการคำนวณด้วยเลขทศนิยมจาก 6 หลักเหลือ 3 หลักโดยคิดว่าเลขทศนิยมที่ตัดทิ้งจะไม่มีนัยสำคัญแต่ผลของการคำนวณ แต่เมื่อเวลาผ่านไปช่วงเวลาหนึ่ง พบว่าผลของการคำนวณด้วยค่าเริ่มต้นด้วยทศนิยม 3 หลัก ได้เปลี่ยนแปลงจากการคำนวณครั้งก่อนไปอย่างมากมายหรือเพียงกำหนดค่าเริ่มต้นต่างกันเล็กน้อยผลของสมการอนุพันธ์ ที่ Lorenz จำลองขึ้นนี้จะให้ผลแตกต่างกันอย่างสิ้นเชิง กล่าวได้ว่าระบบที่จำลองขึ้นนี้ไวต่อค่าเริ่มต้นและเมื่อทำการพล๊อต ความสัมพันธ์ระหว่างตัวแปร x ต่อ y และx ต่อ z จะมีลักษณะรูปร่างที่แปลกประหลาดมีลักษณะเป็นตัวดึงดูดอลวน (attractor)โดย ลักษณะของ x ต่อ z มีลักษณะคล้ายปีกผีเสื้อ และ Lorenz เรียกปรากฏการณ์ที่ค้นพบโดยบังเอิญนี้ว่าผลกระทบของผีเสื้อ (Butterfly effect) โดยให้ความหมายในระบบอุตุนิยมวิทยาว่าเป็นระบบที่อ่อนไหวมากเพียงผีเสื้อขยับปีกที่ Hong Kong ก็อาจเกิดปรากฏการณ์ Tornado หรือสภาวะสับสนอลหม่านที่ California ได้

หลังจากที่ Lorenz ได้ค้นพบตัวดึงดูดอลวนแรกแล้ว ต่อมา Rosslor [2] ได้ค้นพบตัวดึงดูดอลวน จากการจำลองปรากฏการทางเคมี โดยมีเทอมตัวแปรไม่เป็นเชิงเส้นเพียงเทอมเดียว และในขณะต่อมา Rosslor [3] ได้นำเสนอตัวดึงดูดอลวน ขนาด 4 มิติ หรือ ไฮเปอร์เคออสติก โดยการเพิ่มลำดับของสมการจากลำดับ 3 เป็น ลำดับ 4

คุณลักษณะของตัวดึงดูดอลวน [4]

1. มีความไวต่อค่าเริ่มต้น
2. มีลักษณะคล้ายสัญญาณรบกวนในโดเมนของเวลา

3. สเปคตรัมกำลังของสัญญาณมีลักษณะย่านกว้าง

สำหรับการสร้างตัวดึงดูดอลวนในวงการวิศวกรรมไฟฟ้านั้น Chua [5] ได้นำเสนอการสร้างวงจรเพื่อกำเนิด สัญญาณเคออสขึ้นโดยวงจรประกอบด้วย ความต้านทาน 1 ตัว ตัวเก็บประจุ 2 ตัว ความเหนี่ยวนำ 1 ตัวและอุปกรณ์สร้างความต้านทานลบไม่เป็นเชิงเส้น 1 ชุด โดยวงจรนี้ สามารถกำเนิดสัญญาณเคออสได้ทั้งแบบ 1 สกอร์ และ 2 สกอร์ โดยปรับที่ตัวต้านทาน และเราเรียกวงจรที่ Chua ประดิษฐ์ขึ้นว่า วงจรของ Chua (Chua's Circuit) พร้อมขณะเดียวกัน Matsumoto[6] ผู้ที่ทำการร่วมวิจัยกับ Chua ได้นำเสนอวงจรกำเนิดสัญญาณเคออสแบบ 4 มิติ หรือ ไฮเปอร์เคออส ขึ้นจริงโดยสร้างจากวงจรที่มีลักษณะคล้ายวงจรของ Chua โดยเพิ่มลำดับของสมการอนุพันธ์ ด้วยการเพิ่มค่าตัวเหนี่ยวนำ

สำหรับการประยุกต์ใช้งานของ ตัวดึงดูดอลวน นั้น หลังจาก Pecora [7] ได้แสดงให้เห็นว่า ระบบเคออสของ Lorenz และ Rosslor สามารถซิงโครไนซ์ (Synchronization) เข้าด้วยกัน โดยมีภาคส่งเรียกว่า ตัวขับ (drive) และภาครับเรียกว่า ตัวตอบสนอง (Response) แล้ว ต่อมา Cuomo [8] ได้นำเอาหลักการดังกล่าวไปใช้ในการประยุกต์การสื่อสารแบบปลอดภัยโดยนำสัญญาณเสียง ทำการบวกเข้า (masking) กับตัวขับซึ่งเป็นระบบ Lorenz และเมื่อสัญญาณนี้ส่งผ่านไปในช่องสัญญาณ ผู้ดักฟังสัญญาณไม่สามารถฟังได้ ยกเว้นจะมีตัวถอดรหัสหรือภาครับที่สามารถตอบสนองกับสัญญาณเคออสเพื่อจะถอดรหัสออกมาได้ซึ่งระบบที่ Cuomo ได้นำเสนอเป็นการเข้ารหัสลับแบบง่ายๆ ต่อมา Yang [9] ซึ่งเป็นผู้ร่วมวิจัยกับ Chua ได้เพิ่มความแข็งแกร่งของระบบเข้ารหัสลับที่อยู่บนพื้นฐานของระบบเคออสโดยนอกจากใช้การซิงโครไนซ์ของวงจรของ Chua แล้วยังเพิ่มตัวเข้ารหัสลับที่วงจร Chua อีกหนึ่งชุด สำหรับการสื่อสารแบบกระจายสเปคตรัม Itoh [10] ได้นำประโยชน์จากคุณสมบัติที่สัญญาณเคออสมีย่านความถี่กว้างไปประยุกต์เพื่อเป็นคลื่นพาห์ของการกระจายสเปคตรัม และด้วยคุณสมบัติที่สัญญาณเคออสคล้ายสัญญาณรบกวน Yalcin [11] ได้นำเสนอการสร้างการกำเนิดบิตสุ่มจริงจากตัวดึงดูดอลวนโดยการนำการเคลื่อนที่ของวงโคจรของตัวดึงดูดอลวนผ่านจุดสมดุลมากำเนิดบิตสุ่ม

หลังจากการค้นพบวงจรของ Chua ซึ่งมีผู้นำไปประยุกต์ใช้งานดังกล่าวมาแล้ว ได้มีผู้สร้างตัวดึงดูดอลวนแบบใหม่ๆ โดยอาศัยพื้นฐานจากสมการของ Lorenz โดย

Chen [12] ได้ค้นพบตัวดึงดูดอลวนแบบใหม่จากการควบคุมระบบ Lorenz ให้ไม่มีเสถียรภาพ หรือการต่อต้านการควบคุม (anti-control) โดยเราเรียกวิธีการนี้ว่า Chaotification ซึ่งตัวดึงดูดอลวนของ Chen มีเทอมตัวแปรแบบไม่เป็นเชิงเส้น 2 เทอม เช่นเดียวกันกับ Lorenz แต่สัมประสิทธิ์ ของสมการต่างจาก Lorenz และในเวลาต่อมา Lu [13] ซึ่งเป็นผู้ร่วมวิจัยกับ Chen เสนอตัวดึงดูดอลวน ที่แสดงลักษณะเหมือนกับ Lorenz และ Chen ด้วยการปรับพารามิเตอร์โดยขณะเวลาเดียวกันได้มีผู้เสนอการสร้างวงจรสร้างตัวดึงดูดอลวนปีกผีเสื้อแบบ Lorenz[14] โดยใช้เทคนิคการคูณแบบสวิชท์แทนการคูณแบบเชิงเส้น สำหรับการสร้างตัวดึงดูดอลวนแบบง่ายนั้น Sprott [15] ได้เสนอรูปแบบสมการอนุพันธ์ลำดับ 3 รวมกับตัวแปรแบบไม่เป็นเชิงเส้นแบบง่ายๆ ที่สามารถสร้างได้โดยวงจรอิเล็กทรอนิกส์ ซึ่ง สมการของ Sprott ให้กำเนิดรูปแบบตัวดึงดูดอลวนที่มีรูปแบบไม่ซับซ้อนมาก

สำหรับการสร้าง ตัวดึงดูดอลวนที่มีความซับซ้อนเพื่อประยุกต์ใช้ในการเข้ารหัสลับหรือสื่อสารแบบปลอดภัยนั้นได้เริ่มพัฒนาโดย Suyken [16]นำเสนอการสร้าง ตัวดึงดูดอลวน แบบหลายสกอร์ จากวงจรของ Chua ด้วยการเพิ่มท่อนของความต้านทานลบ เพื่อเพิ่มจุดสมดุลในระบบ และ Tang [17] ได้เสนอการสร้างวงจรหลายสกอร์จากวงจรของ Chua เช่นเดียวกัน โดยการสร้างวงจรต้านทานลบเป็นค่าฟังก์ชัน sin(x) สำหรับการสร้างวงจรเพื่อกำเนิดตัวดึงดูดอลวนแบบ 4 มิตินั้น Li [18] ได้นำเสนอการสร้างตัวดึงดูดอลวนแบบไฮเปอร์โดยเพิ่มขนาดลำดับเพื่อควบคุมสมการของ Lorenz โดย Chen [19] และ Lu [20] ได้ใช้เทคนิคแบบเดียวกันเพื่อสร้างตัวดึงดูดอลวนแบบไฮเปอร์จากตัวดึงดูดอลวนของ Lu[13] และตัวดึงดูดอลวนของ Chua [5]แบบหลายสกอร์ตามลำดับ

นอกจากประยุกต์ตัวดึงดูดอลวน สำหรับการสื่อสารแบบปลอดภัย การสื่อสารแบบกระจายสเปคตรัม และการกำเนิดเป็นบิตสุ่มจริงแล้ว ผู้วิจัยได้เสนอการใช้ตัวดึงดูดอลวน สำหรับเป็นการขับเคลื่อนหุ่นยนต์สนาม [22]-[25] และการขับมอเตอร์เพื่อการปั่นผสม [26] ซึ่งหัวใจของการประยุกต์ทั้งหมดคือคือตัวกำเนิดสัญญาณเคออสหรือวงจรสร้างตัวดึงดูดอลวน โดยเฉพาะในการสื่อสารแบบปลอดภัยนั้นจำเป็นต้องสร้างตัวดึงดูดอลวนให้มีค่าซับซ้อนสูงเพื่อยากต่อการสร้างสัญญาณกลับ (reconstruction) สำหรับผู้ดักฟัง โดยการประยุกต์เพื่อใช้งานจริงในรูปแบบต่างๆที่

กล่าวมาผู้วิจัยส่วนใหญ่ได้จดสิทธิบัตรพร้อมกับปกปิดเทคนิคบางอย่างในการสร้าง ดังนั้นเพื่อให้เราสามารถทำงานประยุกต์ใช้งานตัวดึงดูดอลวนหรือระบบไม่เป็นเชิงเส้นสำหรับงานวิศวกรรมได้จริง จำเป็นที่ต้องมีเทคนิคการสร้างวงจรกำเนิดตัวดึงดูดอลวน ของเราเอง ดังนั้นในข้อเสนอโครงการวิจัยนี้จึง เสนอวิธีการสร้างตัวดึงดูดอลวนแบบใหม่ขึ้นเพื่อเป็นต้นแบบในการประยุกต์ใช้งานดังกล่าว

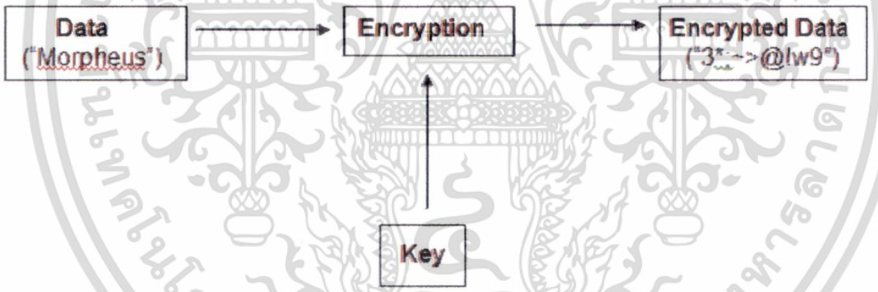
สำหรับหลักการสร้าง ตัวดึงดูดอลวน ในรูปแบบที่ใช้เทคนิคการประมาณเทอมเพื่อให้ได้ตัวดึงดูดอลวนแบบใหม่ซึ่งสามารถทำให้เราสร้างฟังก์ชันท่อนแทนค่าสมบูรณ์ เพื่อใช้สร้างตัวดึงดูดอลวน หลายปีกเป็นการใช้ฟังก์ชันเชิงท่อนที่สร้างขึ้นโดยทางปฏิบัติสามารถสร้างได้ง่ายกว่า ฟังก์ชันเชิงท่อนที่สร้างเป็นค่าความต้านทานลบ[16,17,20] และลักษณะของตัวดึงดูดอลวนยังให้รูปแบบที่ซับซ้อนสูงกว่าแบบอื่นๆ มาก[14,19,20] สำหรับตัวดึงดูดอลวนแบบที่ 3 ที่ได้สร้างขึ้นแบบตัวดึงดูดอลวนแบบหลายสกอร์ สร้างขึ้นจากตัวดึงดูดอลวนซึ่งมีจุดสมดุลย์เพียงจุดเดียว ทำให้การโคจรของตัวดึงดูดอลวนวงนอกมีลักษณะลดลงแบบ expentent ซึ่งจะต่างกับตัวดึงดูดอลวนแบบอื่นๆ[16,17,18,19,20] ที่ได้นำเสนอ และสำหรับตัวดึงดูดอลวน แบบสุดท้ายนั้นใช้หลักการ chaotification และร่วมกับการป้อนกลับทำให้ได้ attractor ที่มีค่า Lyapunov ที่สูง

ในงานวิจัยที่จะนำเสนอนี้จะเป็นการใช้เทคนิคดังที่กล่าวมาแล้วในข้างต้นเพื่อค้นหาสภาวะอลวนแบบใหม่ที่ให้ความแข็งแกร่งและคงทนตามวัตถุประสงค์ดังกล่าวแล้วและประยุกต์สัญญาณอลวนในระดับที่สามารถสร้างอุปกรณ์ได้ [27] ผลการสร้างเครื่องมือพื้นฐาน (primitive tools) แสดงในบทที่ 3

บทที่ 3 วิธีดำเนินการวิจัยและผลการวิจัย

3.1 การสร้างสัญญาณอลวนแบบใหม่

ผู้วิจัยและคณะได้ออกแบบสถาปัตยกรรมของการเข้ารหัสภาพที่ได้จากตาหุ่นยนต์ โดยในช่วงเฟสแรกผู้วิจัยและคณะมุ่งเน้นการตรวจสอบอัลกอริธึมของการเข้ารหัสจึงมุ่งเน้นการเข้ารหัสภาพนิ่งเป็นเบื้องต้น โดยอาศัยวิธีการเข้ารหัสในเอกสารและอัลกอริธึมและได้ขยายผลที่ได้นี้ต่อไปโดยใช้สัญญาณอลวนแบบร่วมสามารถกระทำการผสมสัญญาณที่กล่าวไว้ในเอกสารดังหมายเลข [27] ในหมวดบรรณานุกรม อย่างไรก็ตาม แนวคิดรวบยอดที่ใช้นี้ใช้สถาปัตยกรรมเดียวกันดังแสดงสังกัปหรือแนวคิดรวบยอดได้ดังรูปที่ 2 ซึ่งใช้กุญแจรหัสที่สร้างขึ้นโดยผู้ใช้เพื่อเปลี่ยนข้อมูลที่ต้องการส่งให้เป็นข้อมูลที่ใส่รหัสลับ (cipher) ให้เป็นข้อมูลที่ดูด้วยสายตาเสมือนไม่มีความสัมพันธ์กัน



รูปที่ 2 แผนภาพขั้นตอนแนวคิดการใช้กุญแจรหัสสำหรับการเข้ารหัส

ในการเข้ารหัสลับภาพโดยทั่วไปนั้นจะแตกต่างจากส่วนที่เป็นอักษร ด้วยเหตุว่าภาพจุข้อมูลมากกว่า (bulk capacity) มีข้อมูลซ้ำมากกว่า (high redundancy) และมีค่าสหสัมพันธ์ระหว่างพิกเซลสูง (high correlation) ด้วยคุณสมบัติดังกล่าวนี้การประมวลผลภาพโดยใช้วิธีการเข้ารหัสแบบดั้งเดิมที่ใช้กันโดยทั่วไปนั้นใช้เวลาในการเข้ารหัสค่อนข้างนาน ดังนั้นในงานวิจัยนี้ ใช้วิธีการเข้ารหัสแบบใช้สัญญาณอลวนเพื่อสร้างความมั่นคงปลอดภัยของข้อมูลโดยใช้สัญญาณอลวน ในการการเข้ารหัสลับ จะนำสัญญาณข้อมูลที่จะส่งหรือเก็บเข้ารหัสด้วยขบวนการทางคณิตศาสตร์กับสัญญาณ

อลวนก่อน และในการถอดรหัสลับเพื่อให้ได้สัญญาณรูปแบบเดิมกลับมาจะเป็นการกระทำกลับ (inverse) โดยใช้สัญญาณอลวนเช่นกัน ดังนั้นในงานวิจัยนี้จึงต้องหารูปแบบสัญญาณอลวนในรูปแบบใหม่ๆขึ้นมาเพื่อให้ยากต่อบุคคลที่3 ที่ต้องการถอดรหัส และหลังจากได้รูปแบบสัญญาณอลวนที่ซับซ้อนแล้วจึงจะทำการสร้างต้นแบบเครื่องเข้ารหัสข้อมูลลับ โดยในงานวิจัยนี้จะสร้างเครื่องตนแบบสำหรับการประยุกต์ 3 รูปแบบคือ

1. สร้างอุปกรณ์เพื่อแสดงตน (Authentication)
2. สร้างอุปกรณ์เข้ารหัสของภาพแบบ Offline
3. สร้างอุปกรณ์เข้ารหัสแบบ Online

โดยมีรายละเอียดดังนี้

1.การสร้างอุปกรณ์แสดงตนนั้นจะเป็นการนำเอาสัญญาณที่เป็นรหัสแสดงตนทำการผสมกับสัญญาณอลวน และนำเอาสัญญาณที่ผสมแล้วนี้เข้าสู่คอมพิวเตอร์ซึ่งทำหน้าที่พิสูจน์ตน

2.การสร้างอุปกรณ์เข้ารหัสของภาพหรือเอกสารแบบ Offline เป็นการเข้ารหัสลับของภาพหรือเอกสารที่อยู่บนคอมพิวเตอร์โดยนำเอาเอกสารทำการเข้ารหัสกับสัญญาณอลวนที่สร้างขึ้นโดยสัญญาณอลวนจะถูกสร้างขึ้นโดยวงจรและส่งเข้าสู่คอมพิวเตอร์จากการเชื่อมต่อแบบ USB

3.การสร้างอุปกรณ์เข้ารหัสเสียงแบบ Online จะเป็นการทำการเข้ารหัสลับของเสียงที่จะส่งไปในช่องสัญญาณโทรศัพท์ กับสัญญาณอลวนโดยรูปแบบนี้จะทำการเข้ารหัสแบบเวลาจริง (Real time) โดยที่ภาครับสามารถจะทำการถอดรหัสได้ทันที

ดังนั้นหัวใจของการสร้างอุปกรณ์ทั้ง 3 รูปแบบคือการสร้างสัญญาณอลวนที่มีความซับซ้อนยากต่อการถอดรหัสแก่บุคคลที่3 และต้องเป็นรูปแบบสัญญาณที่ยังไม่เคยมีปรากฏมาก่อนหน้านี้ด้วย โดยรูปแบบสัญญาณอลวนที่ปรากฏอยู่ในเอกสารงานวิจัยทั่วไปมีอยู่ 2 แบบคือ

1. แบบกำเนิดด้วยตนเอง (Autonomous Chaotic Oscillator)
2. แบบกำเนิดด้วยการกระตุ้นจากภายนอก (Non Autonomous Chaotic Oscillator)

โดยทั้งสองแบบนั้นมีวงจรเป็นที่รู้จักคือวงจร Chua [5] และมีรูปแบบอื่นๆ ที่สร้างโดยตรงจากสมการอลวนได้คือวงจรสร้างจากสมการของ Lorenz [1] วงจรสร้างจาก

สมการของ Chen [4] หรือวงจรแบบหลายสกอร์ [4] แต่วงจรอลวนที่กล่าวมาแล้วนั้น ยังมีความซับซ้อนของสัญญาณค่อนข้างต่ำเมื่อวัดจากการสร้างกับโดยใช้อนุกรมทางเวลาดังนั้นในงานวิจัยนี้ในระยะแรกจึงทำการสร้างวงจรอลวนแบบซับซ้อนขึ้นเพื่อนำไปประยุกต์ใช้กับเป้าหมายที่กล่าวมา

สำหรับงานวิจัยที่ได้ดำเนินการไปแล้วคือ การสร้างสัญญาณอลวนที่รูปแบบซับซ้อน ซึ่งเป็นการค้นพบใหม่อยู่ 2 รูปแบบคือ

1. สัญญาณอลวนแบบผีเสื้อหลายปีก
2. สัญญาณอลวนแบบกำเนิดด้วยคลื่นกระตุ้นหลายปีก

สำหรับการสร้างสัญญาณอลวนแบบผีเสื้อหลายปีกได้ปรับปรุงมาจากวงจรอลวนปีกผีเสื้อของ LUI ซึ่งสมการนี้มีลักษณะคล้ายสมการของ Lorenz แต่ในเทอมที่ไม่เป็นเชิงเส้น สามารถปรับปรับให้มีรูปแบบที่ซับซ้อนได้ง่ายโดยสมการของ LUI แสดงได้คือ

$$\begin{aligned} x' &= -ax + ay \\ y' &= bx - kxz \\ z' &= -cz + hx^2 \end{aligned}$$

โดยค่า $a = 10, b = 40, c = 2.5, h = 4, k = 1$ เป็นค่าคงที่

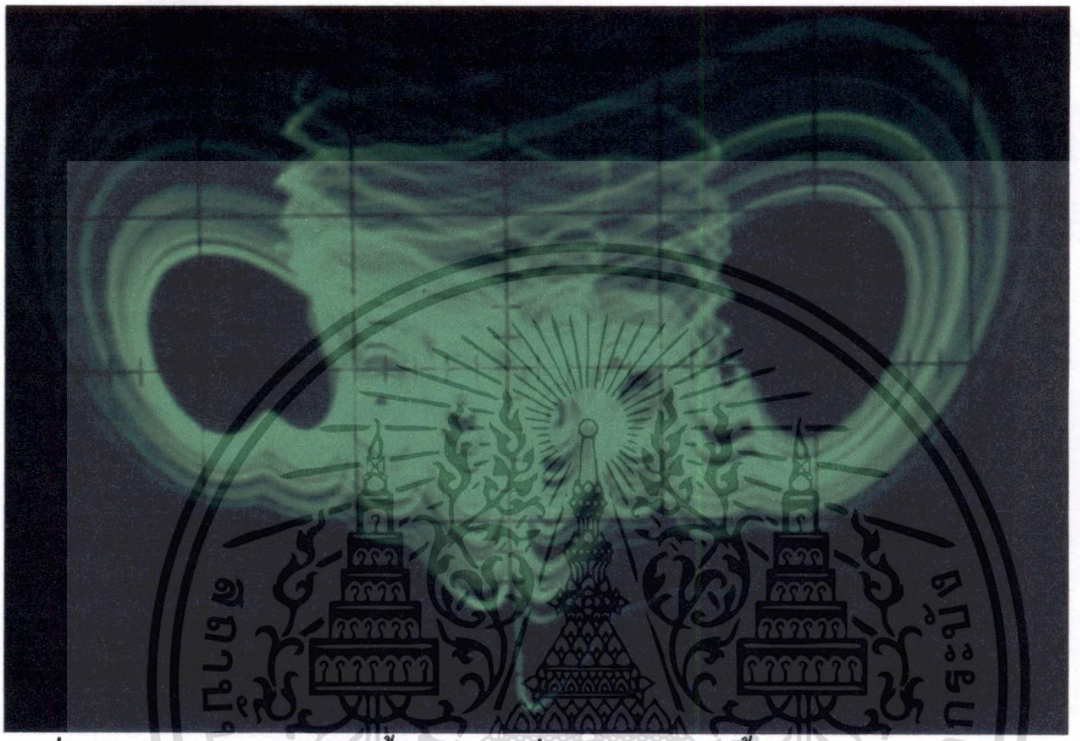
ในการเคลื่อนที่ของวงโคจรสัญญาณอลวนระหว่างจุดสมดุลย์สองจุดในมิติ 3 ระนาบ ดังนั้นในการเพิ่มความซับซ้อนของสัญญาณเคออสกระทำได้โดยเพิ่มจุกสมดุลย์ในระบบ หรือปรับปรุงฟังก์ชันไม่เป็นเชิงเส้น x^2 ให้มีค่า f(x) หรือสมการผีเสื้อหลายปีกที่พบใหม่ได้คือ

$$\begin{aligned} x' &= -ax + ay \\ y' &= bx - k_1 xz \\ z' &= -cz + hf(x) \end{aligned}$$

โดยค่า $f(x)$ แสดงได้คือ $$f(x) = |x| + \sum_{i=1}^{m} \left(1 + \frac{1}{2}\mathrm{sgn}(x-i) - \frac{1}{2}\mathrm{sgn}(x-i)\right)$$

โดยในการพิสูจน์ว่าสัญญาณอลวนสามารถกำเนิดได้จริง ได้ทำการทดลองสร้างขึ้นโดยใช้วงจรอิเล็คทรอนิกส์

โดยมีผลการทดลองดังรูปที่ 3



รูปที่ 3 สัญญาณอลวนแบบผีเสื้อหลายปีกที่พบในงานวิจัยนี้

2. การสร้างสัญญาณอลวนแบบกำเนิดด้วยคลื่นกระตุ้นหลากวงทำการปรับปรุงจากสมการ

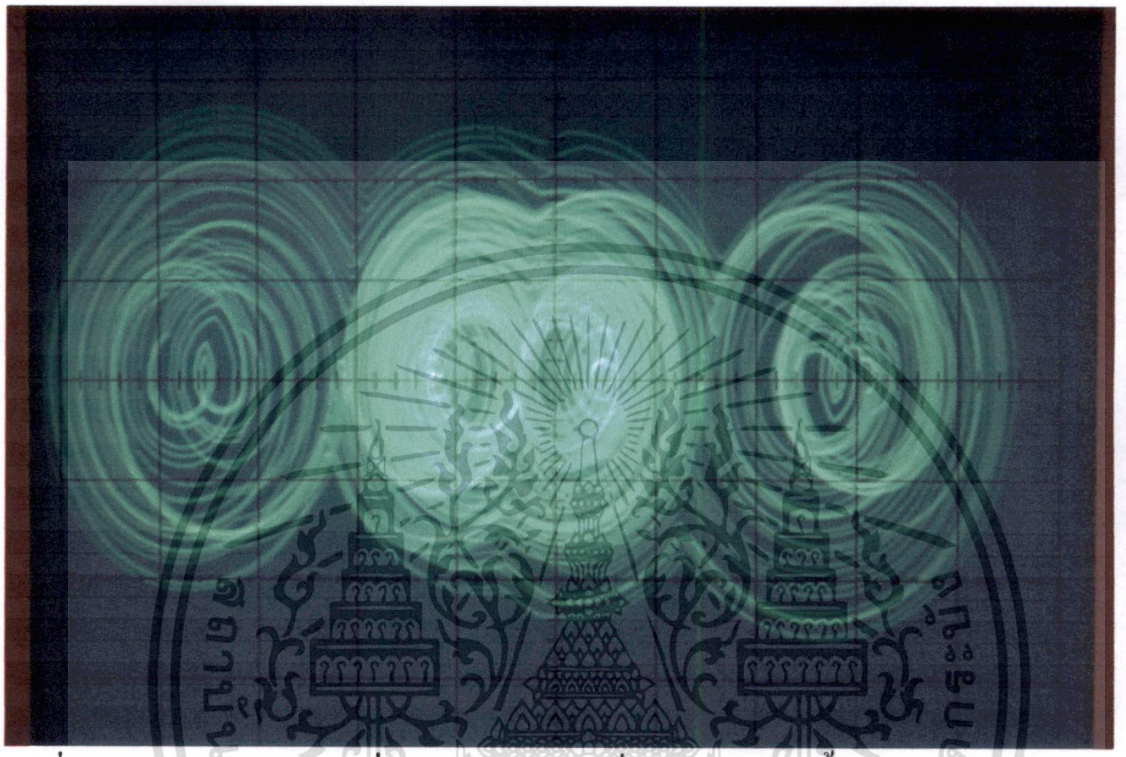
$$x' = -ax + by$$
$$y' = -x + k \cdot \mathrm{sgn}(x) + A\sin(\omega t)$$

ให้มีรูปแบบหลายวงโดย

$$x' = -ax + by$$
$$y' = -x + k \cdot f(x) + A\sin(\omega t)$$

โดย $f(x) = \sum_{i=1}^{m} \left(\frac{1}{2}\mathrm{sgn}(x+i) + \frac{1}{2}\mathrm{sgn}(x-i) \right)$

ผลการทดลองพบดังรูปที่ 4



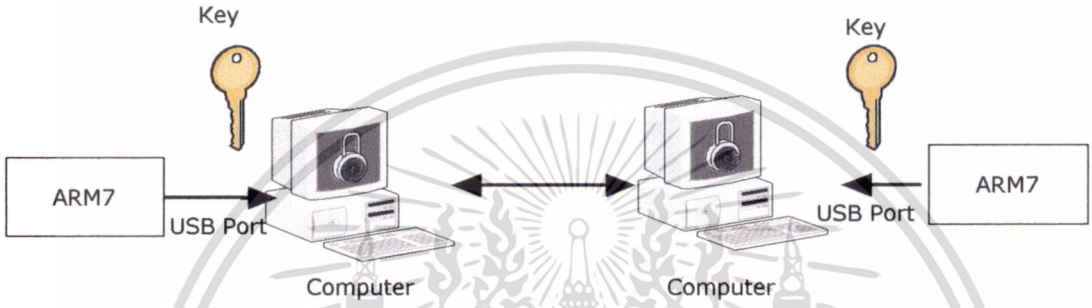
รูปที่ 4 สัญญาณอลวนแบบคลื่นกระตุ้นหลากวงที่พบในงานวิจัยนี้

เพื่อความแข็งแกร่งในการเข้ารหัสลับตาหุ่นยนต์ซึ่งในเฟสแรกเป็นการทดลองในกรณีภาพนิ่ง จะใช้อุปกรณ์เข้ารหัสแบบฮาร์ดแวร์ร่วมกับซอฟท์แวร์ โดยในส่วนของฮาร์ดแวร์ในเบื้องต้นนี้ใช้ไมโครคอนโทรลเลอร์

ที่มีความเร็วสูง (high-speed secure microcontroller) มาใช้เป็นตัวควบคุมการเข้ารหัสผ่านพอร์ต Universal Serial Bus: USB. โดยฮาร์ดแวร์ดังกล่าวใช้เป็นตัวสร้างสายธารกุญแจรหัสลับที่เชื่อมต่อกับคอมพิวเตอร์โดยมีการเชื่อมต่อกุญแจรหัสส่วนฮาร์ดแวร์ที่พอร์ต USB ผู้ได้รับอนุญาติให้ร่วมตรวจสอบการใช้ภาพและเอกสารจะใช้รหัสลับของตนเข้ารหัสหรือถอดรหัสภาพที่ได้ต่อไป ดังจะแสดงผลการวิจัยเพิ่มเติมที่ได้ในหัวข้อถัดไป สำหรับรูปแบบสัญญาณอลวนที่ค้นพบใหม่เพิ่มเติมดูได้จากภาคผนวก

3.2 การออกแบบ

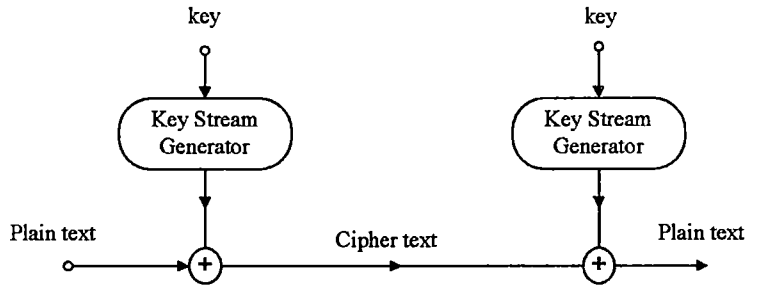
การสร้างอุปกรณ์เข้ารหัสของภาพหรือเอกสารแบบ Offline เป็นการเข้ารหัสลับของภาพหรือเอกสารที่อยู่บนคอมพิวเตอร์โดยนำเอาเอกสารทำการเข้ารหัสกับสัญญาณอลวนที่สร้างขึ้นโดยสัญญาณจะถูกสร้างขึ้นโดยไมโครคอนโทรเลอร์ ARM 7 และส่งเข้าสู่คอมพิวเตอร์จากการเชื่อมต่อแบบ USB



รูปที่ 5 ขั้นตอนการออกแบบและการเข้ารหัสลับ

ในขั้นตอนออกแบบระบบเข้ารหัสลับแบบสตีม(Stream cipher)นี้ ซึ่งมีโครงสร้างดังรูปที่ 6 เรียกว่า Vernam หรือ One time pad cipher [28,29] โดยข้อมูลที่จะเข้ารหัสลับเรียกว่า plaintext จะถูกนำมา EX –OR กับคีย์สตีมที่กำเนิดจาก USB (Keystream) ที่กำหนดรูปแบบได้โดยค่ากุญแจ (Key) สำหรับผลของการ EX-OR ที่ได้เรียกว่าCipher Text สำหรับคีย์สตีมต้องมีคุณสมบัติ ดังนี้

1. มีคุณสมบัติทางสถิติที่ดี
2. ง่ายต่อการสร้าง
3. สามารถทำงานที่บิตเรตสูงๆ
4. มีความปลอดภัยจากการค้นหาจาก Cipher text



รูปที่ 6 ระบบเข้ารหัสลับแบบสตีม

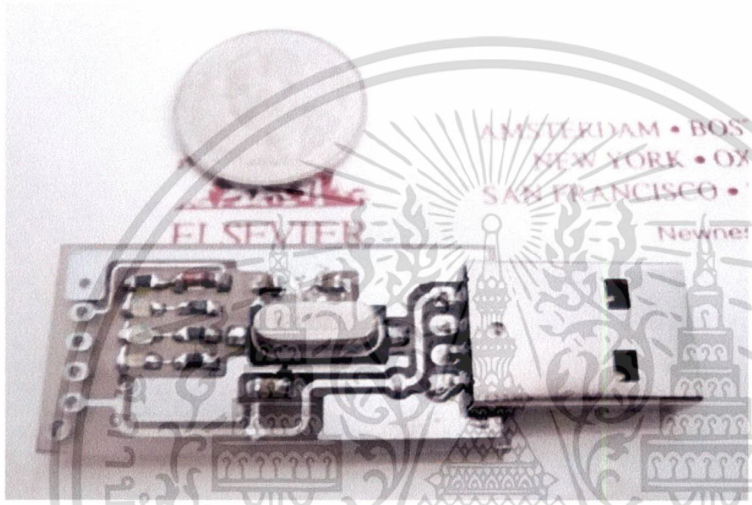
สำหรับเงื่อนไขของระบบเข้ารหัสที่ดี Shannon ได้มีข้อกำหนดถึงนิยาม คือ Confusion หมายถึง plain text ต่อ cipher text ต้องไม่มีความสัมพันธ์ทางสถิติหรือผลของ Cipher text ต้องไม่ขึ้นอยู่กับ Plain text Diffusion การเปลี่ยนแปลง Plain text เพียงเล็กน้อยต้องมีผลต่อการเปลี่ยนแปลง cipher text อย่างมาก ดังนั้นจากคุณสมบัติของเคออส ที่มีความไวต่อการเปลี่ยนแปลงต่อค่าเริ่มต้นนั้นสอดคล้องกับคุณสมบัติ diffusion ดังนั้นจึงสามารถนำเอาฟังก์ชันเคออสที่มีคุณสมบัติเป็นระบบ Deterministic คือ พฤติกรรมจะเกิดรูปแบบเดิมทุกครั้งจากค่าเริ่มต้นเดียวกันมาสร้างเป็นคีย์สตีม ที่สามารถกำหนดรูปแบบการเกิดได้โดย กำหนด กุญแจด้วยค่าเริ่มต้นของระบบเคออส

จากระบบได้นำระบบเคออสที่ค้นพบใหม่ 3 ระบบมาสร้างสมการเชิงอนุพันธ์สามัญจากนั้นจึงสุ่มค่าเป็นค่าคีย์สตีมและทำการทดสอบความเป็นค่าสุ่มก่อนที่จะเขียนโปรแกรมลงบนไมโครคอนโทรเลอร์ ARM 7 โดยใช้ผลจากระบบสมการอลวนที่ได้ในบทที่ 3 โดยใช้การคำนวณโดยระเบียบวิธีการแก้สมการเชิงอนุพันธ์สามัญหลายรูปแบบ ในที่นี้ใช้ 4 วิธี คือ

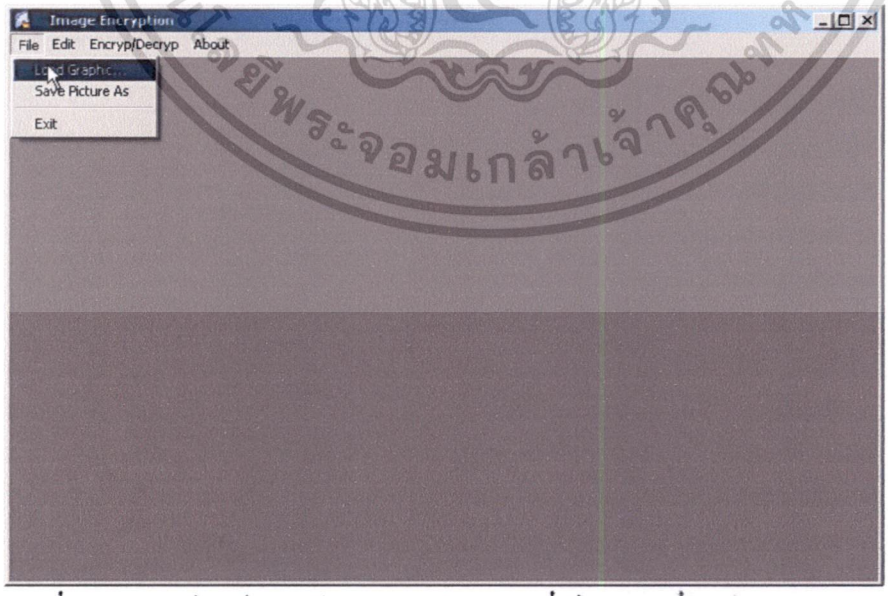
1. ระเบียบวิธีของออยเลอร์ (Euler's method)
2. ระเบียบวิธีของฮวน (Heun 's method)
3. ระเบียบวิธีของออยเลอร์ที่ปรับปรุงแล้ว (Modified Euler's method)
4. ระเบียบวิธีของรุงเง-คุตตา (Runge-Kutta method)

3.3 การทดลองชิ้นงานกุญแจรหัส

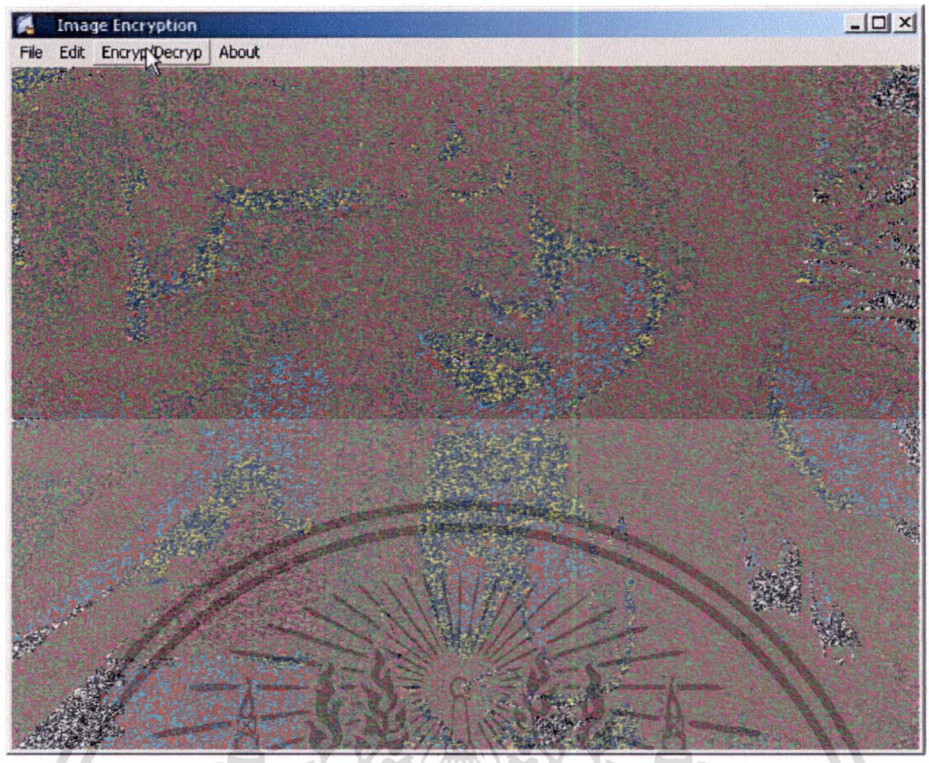
กุญแจรหัสในส่วนภาพนิ่งเบื้องต้น โดยอาศัยเทคนิคการสอดสัญญาณอลวน โดยอาศัยการสร้างธารกระแสข้อมูลรหัสโดยไมโครคอนโทรลเลอร์ที่ได้ออกแบบและสร้างในส่วนนี้ได้แสดงดังรูปที่ 7 โดยใช้ร่วมกับซอฟท์แวร์ในรูปที่ 8 รูปที่ 9 ภาพทดสอบการทำงานของอุปกรณ์ที่ได้ออกแบบและรูปที่ 10 เป็นภาพที่ได้จากการเข้ารหัสลับแล้ว



รูปที่ 7 กุญแจรหัสลับสำหรับเข้ารหัสลับผ่านพอร์ต USB



รูปที่ 8 ซอฟท์แวร์การเข้ารหัสลับในส่วนที่เป็นภาพนิ่งใช้ร่วมกับอุปกรณ์กุญแจรหัสในรูปที่ 7 ผ่านพอร์ต USB



รูปที่ 9 ภาพที่ได้จากการเข้ารหัสลับของรูปที่ 7 แล้ว

บทที่ 4 อภิปรายผลการวิจัยและวิจารณ์

ในการทดสอบความแข็งแกร่งของรหัสลับอลวนในงานวิจัยนี้นั้น ใช้การทดสอบบิตที่เกิดขึ้นในงานวิจัยนี้ใช้ตามข้อกำหนดของ NIST แบบ FIPS 140-2 [30] มีการทดสอบอยู่ 4 รูปแบบ คีย์สตีมที่สามารถใช้ในการเข้ารหัสลับได้ต้องผ่านการทดสอบทั้ง 4 รูปแบบ สำหรับการทดสอบทำการทดสอบคีย์สตีมจำนวน 20,000 บิตมีดังนี้คือ

1. การทดสอบ Mono bit เป็นการทดสอบการเกิดบิต 1 ถ้าให้ X เป็นการเกิดบิต 1 แล้วข้อกำหนดของคีย์สตีมที่ผ่านการทดสอบคือ $9,725 < X < 10,275$ บิต

2. การทดสอบ Poker เป็นการทดสอบโดยการแบ่งบิตจำนวน 20,000 บิตออกเป็นกลุ่มของบิตติดกันจำนวน 4 บิต(ซึ่งมีอยู่ 16 รูปแบบ) จำนวน 5,000 กลุ่ม ทำการนับจำนวนรูปแบบทั้งหมดที่เกิดขึ้น ถ้าให้ $f(i)$ เป็นจำนวนค่าของแต่ละรูปแบบแล้วหาค่า

$$X = \frac{16}{5000}\sum_{i=1}^{n}|f(i)|^2 - 5,000 \qquad (11)$$

โดยข้อกำหนดของคีย์สตีมที่ผ่านการทดสอบคือ $2.16 < X < 46.17$

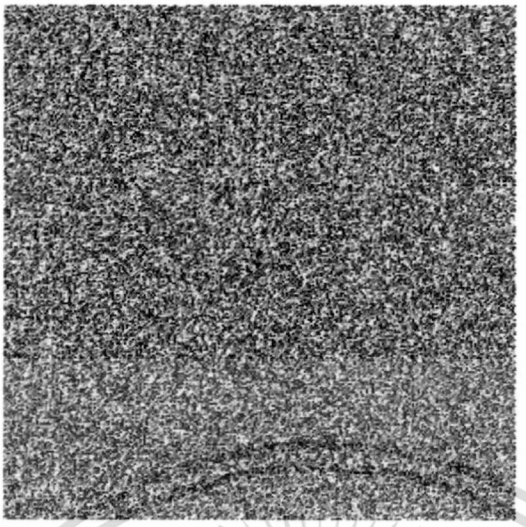
3. การทดสอบ Run เป็นการทดสอบเกิดบิต 1 ที่ติดกันของบิตทดสอบจำนวน 20,000 บิต ข้อกำหนดของบิตที่ผ่านการทดสอบคือ

จำนวนบิต 1 ติดกัน	ต้องอยู่ในช่วง
1	2,315- 2,685
2	1,114-1,386
3	524 - 723
4	240- 384
5	103- 209
6+	103-209

4. การทดสอบ Long run เป็นการทดสอบบิตจำนวน 20,000 บิตต้องไม่มีบิต 0 หรือ 1 ติดกันเกิน 25 บิต

ตัวอย่างผลการทดลอง ของเข้ารหัสลับของไฟล์ภาพด้วยสมการอลวนด้วยระบบที่สร้างขึ้นและผ่านการทดสอบดังกล่าวข้างต้นแสดงเชิงคุณภาพดังรูปที่ 10 และ 11 ดังนั้นระบบที่สร้างขึ้นนี้มีความเชื่อมั่นในระดับที่ผ่านการทดสอบตามข้อกำหนด NIST

รูปที่ 10 Plain image



รูปที่ 11 Cipher image

บทที่ 5 สรุปและข้อเสนอแนะ

งานวิจัยนี้เสนอและพิสูจน์แนวคิดในการเข้ารหัสลับไฟล์ต่าง ๆ ซึ่งในงานวิจัยนี้ได้ใช้สัญญาณอลวนในการเข้ารหัสลับ ในเฟสแรกของการวิจัยที่พิสูจน์ตัวตนโดยการเข้ารหัสลับในระบบข้อมูลแบบสถิต (statics) ผลการเข้ารหัสลับโดยอาศัยอุปกรณ์ฮาร์ดล็อกและซอฟท์แวร์ทั้งสองส่วนร่วมกันได้ผลในการกระจายค่าสหสัมพันธ์ของสื่อที่เข้ารหัสจนไม่อาจจะระบุความหมายจากต้นแบบได้

ผลการใช้วิธีดังกล่าวกับระบบพหุสื่อที่เป็นข้อมูลแบบพลวัต (dynamics) ได้ผลเป็นที่น่าพอใจโดยแสดงให้เห็นว่าการถอดรหัสลับแบบอลวนที่ใส่ค่าเงื่อนไขเริ่มต้นผิดให้ผลทำให้ไม่สามารถถอดรหัสได้สำเร็จแม้จะเดารหัสลับได้ใกล้เคียงมากก็ตามดังอภิปรายผลแสดงในบทที่ 4

ผลที่ได้จากการวิจัยนี้สร้างความเชื่อมั่นในศักยภาพสูงที่จะประยุกต์และขยายผลการวิจัยนี้กับทางการทหาร ซึ่งกองทัพไทยควรจะมีรูปแบบการเข้ารหัสลับของตนเองแทนที่จะซื้อหรือพึ่งพาจากต่างประเทศเพราะ “เทคนิคการเข้ารหัสลับ” จัดเป็น “ยุทธปัจจัย” นอกจากนี้ การเข้ารหัสลับในชั้นที่ไม่ซับซ้อนมากนักเช่น การใช้งานเชิงพาณิชย์นั้น สามารถนำไปใช้ได้เพียงปรับเปลี่ยนรูปลักษณ์และดัดแปลงจากงานวิจัยนี้เพียงเล็กน้อยเท่านั้น ผลงานที่ได้จะส่งมอบให้กับหน่วยงานความมั่นคงในสามจังหวัดชายแดนภาคใต้ร่วมกับผลงานในเฟสที่สอง

บรรณานุกรม

[1] E. N. Lorenz, "Deterministic non-periodic flow," *J. Atmospheric Science*, vol. 20, pp. 130-141, 1963.

[2] O.E. Rössler, "An equation for continuous chaos," *Phys. Lett. A*, vol. 57, pp. 397–398, 1976.

[3] O.E. Rössler, "An equation for hyperchaos," *Phys. Lett. A*, vol. 71, pp. 155–157, 1979.

[4] G. Chen and X. Dong, From Chaos to Order: Methodologies, Perspectives and applications, World Scientifics, Singapore, 1998.

[5] L.O. Chua, M. Komuro and T. Matsumoto, "The double scroll family," *IEEE Trans Circuits Syst.*, vol. 33 , pp. 1072–1118, 1986.

[6] T. Matsumoto, L.O. Chua and K. Kobayashi, "Hyperchaos: laboratory experiment and numerical confirmation," *IEEE Trans Circuits Syst.*, vol. 33 , pp. 1143–1147, 1986.

[7] L.M. Pecora and T.L. Carroll, "Synchronization in chaotic systems," *Phys. Rev. Lett.*, vol. 64, pp. 821–823, 1990.

[8] K.M. Cuomo and A.V. Oppenheim, "Circuit implementation of synchronized chaos with applications to communication," *Phys. Rev. Lett.*, vol. 71, pp. 65–68, 1993.

[9] T. Yang, C.W. Wu and L.O. Chua, Cryptography based on chaotic systems, *IEEE Trans. Circuits Syst.-I: Fundam. Appl.*, vol. 44 , pp. 469–472, 1977.

[10] M. Itoh, "Spread spectrum communication via chaos," *Int. J. Bifurcation Chaos*, vol. 9, pp. 155–213, 1996.

[11] M.E. Yalçin, J.A.K. Suykens and J. Vandewalle, "True random bit generation from a double scroll attractor," *IEEE Trans. Circuits. Syst.- I*, vol. 51 , pp. 1395–1404, 2004.

[12] G. Chen, and T. Ueta, "Yet another chaotic attractor," *Int. J. Bifurcation Chaos*, vol. 9, pp. 1465-1466, 1999.

[13] J. Lü, G. Chen, D. Cheng and S. Čelikovský, "Bridge the gap between the Lorenz system and the Chen system," *Int. J. Bifurcation Chaos*, vol. 12, pp. 2917–2926, 2002.

[14] A.S. Elwakil, S. Özogus and M.P. Kennedy, "Creation of a complex butterfly attractor using a novel Lorenz-type system", *IEEE Trans. Circuits Syst.-I*, vol. 49, pp. 527–530, 2002.

[15] J.C. Sprott, "Simple chaotic systems and circuits", *Am. J. Phys.*, vol. 68 pp. 758–763, 2000.

[16] J.A.K. Suykens, A. Huang and L.O. Chua, A family of *n*-scroll attractors from a generalized Chua's circuit," *AEU. Int. J. Electron. Commun.*, vol. 51, pp. 131–138, 1997.

[17] K.S. Tang, G.Q. Zhong, G. Chen and K.F. Man, "Generation of *n*-scroll attractors via sine function, " *IEEE Trans. Circuits Syst.-I*, vol. 48, pp. 1369–1372, 2001.

[18] Y. Li, W.K.S. Tang and G. Chen, "Hyperchaos evolved from the generalized Lorenz equation," *Int. J. Circuit Theory Appl.*, vol. 33, pp. 235–251, 2005.

[19] A. M. Chen, J. A. Lu, J. Lü and S. M. Yu, "Generating hyperchaotic Lü attractor via state feedback Control," *Physica A*, vol. 364, pp.103-110, 2006.

[20] S. M. Yu, J. Lü and G. Chen, "A family of n-scroll hyper-chaotic attractors and its realizations," *Phys. Lett. A*, 2007, vol. 364, 244-251, 2007.

[21] K. Klomkarn and P. Sooraksa, "Implement of A true Random Number Generator Using Chen's Attractor," *Proc. Int. Conf. Robot, Vision, Information,and Signal Processing*, pp.781-784, 2005.

[22] A. Jansri, K. Klomkarn an P.Sooraksa, "Further investigation on trajectory of chaotic guiding signals for robotic systems," *Proc. Int. Symp. IEEE Communications and Information Technology*, pp.1166 – 1170, 2004.

[23] A.Jansri, K. Klomkarn and P. Sooraksa, "On comparison of attractors for chaotic mobile robots," *Proc. IEEE Industrial Electronics Society*, pp. 2536 – 2541, 2004.

[24] K. Klomkarn and P. Sooraksa, "Implementation on "NO CPU" Chaotic robot," *Proc. the 5th Asian Symposium on Applied Electromagnetics and Machanics*, 2005.

[25] C. Chanvech, K. Klomkarn and P.Sooraksa, "Combined Chaotic Attractor Mobile Robots,"*Int. Joint Conf. SICE-ICASE*, pp. 3079 – 3082, 2006.

[26] S. Sakorntanant, K. Klomkarn, T. Thossansin, and P. Sooraksa, "Chaotic Mixing Biodiesel," *Inter. Conf. on Applied Science*, Vientiane, Loas, 2006.

[27] Sooraksa, P. and Klomkarn, K., An Authentication Device, World Intellectual Property Organization, WO 2008/044998 A1.

[28] A. J. Menezes, P. V. Oorschot, and Vanstone, Handbook of Applied Cryptography. Boca Raton,FL: CRC press, 1997.

[29] C. E. Shannon, "Communication theory of secrecy systems," Bell System Technical Journal, vol. 28, no 4, pp.656—715, Oct. 1949.

[30] National Institute of Standards and Technology, Federal Information Processing Standard Publication FIPS 140-2: Security requirements for cryptographic module, 2001.

ภาคผนวก สัญญาณอลวนที่ค้นพบใหม่เพิ่มเติมในงานวิจัยนี้

ในภาคผนวกนี้ จุดประสงค์การแสดงภาพสัญญาณจากออสซิลโลสโคป จะไม่แสดงชื่อรูป แต่จะแสดงเพียงกระสวนอลวนเท่านั้น ผู้วิจัยขอสงวนสิทธิในการเผยแพร่ เนื่องจากเอกสารนี้เกี่ยวเนื่องกับความมั่นคงของชาติ